ICS 35.020
CCS M 10

中华人民共和国通信行业标准

YD/T XXXX—202X

5G 数据安全评估规范

Specification for 5G data security assessment

（报批稿）

XXXX - XX - XX 发布　　XXXX - XX - XX 实施

中华人民共和国工业和信息化部　发布

目　次

前　言.....1
1 范围.....2
2 规范性引用文件.....2
3 术语和定义.....3
4 略缩语.....3
5 概述.....4
5.1 评估总体框架.....4
5.2 评估原则.....4
5.3 评估启动条件.....5
5.4 评估实施流程.....5
6 5G 业务数据安全评估.....8
6.1 5G 业务通用数据安全.....8
6.2 5G 垂直行业数据安全.....8
7 MEC 数据安全评估.....9
7.1 MEC 平台.....9
7.2 安全域划分和隔离.....9
7.3 MEC 应用环境.....9
7.4 边缘云及数据中心.....10
8 NFV/SDN 数据安全评估.....10
8.1 安全域划分和隔离.....10
8.2 认证.....12
8.3 数据存储.....13
8.4 数据传输.....13
8.5 数据销毁.....13
9 网络切片数据安全评估.....14
9.1 切片管理.....14
9.2 切片隔离.....14
9.3 切片使用.....15
10 核心网基础防护能力评估.....16
10.1 信令保护.....16
10.2 个人敏感信息.....16

10.3 密钥保护.....16
10.4 接口调用.....17
10.5 服务注册发现授权.....17
11 终端设备数据安全评估.....17
11.1 接入安全.....17
11.2 通信安全.....17
11.3 数据存储.....18
11.4 其他.....18
12 无线接入数据安全评估.....18
12.1 机密性保护.....18
12.2 完整性保护和抗重放保护.....18
13 5G基础设施数据安全评估.....19
13.1 物理安全.....19
13.2 云平台安全.....19
13.3 网络安全.....20
14 5G通用数据安全评估.....20

前　言

本文件按照GB/T 1.1-2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利，本文件的发布机构不承担识别专利的责任。

本文件由中国通信标准化协会提出并归口。

本文件起草单位：中国信息通信研究院、中讯邮电咨询设计院有限公司、华为技术有限公司、中国移动通信集团有限公司。

本文件主要起草人：张琳琳、朱纯超、孙宁宁、贾雪瑞、李臣勋、俞小凡、江为强、叶荣伟、王腾。

5G 数据安全评估规范

1 范围

本文件描述了 5G 数据安全评估的原则、范围对象、评估流程，规定了 5G 数据安全评估的评估要点和评估方法。

本文件适用于在通信行业中开展的5G数据安全评估活动，可用于指导5G网络运营者、5G技术业务提供者和使用者开展5G数据安全自评估，也可用于第三方机构等开展5G数据安全评估。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 21052-2007 信息安全技术 信息系统物理安全技术要求

GB/T 25069-2010 信息安全技术 术语

GB/T 31167-2014 信息安全技术 云计算服务安全指南

GB/T 31168-2014 信息安全技术 云计算服务安全能力要求

GB/T 34977-2017 信息安全技术 移动智能终端数据 存储安全技术要求与测试评价方法

GB/T 37092-2018 信息安全技术 密码模块安全要求

GB/T 35273-2020 信息安全技术 个人信息安全规范

YD/T 1729-2008 电信网和互联网安全等级保护实施指南

YD/T 1734-2009 移动通信网安全防护要求

YD/T 2407-2013 移动智能终端安全能力技术要求

YD/T 2692-2014 电信和互联网用户个人电子信息保护通用技术要求和管理要求

YD/T 3169-2020 互联网新技术新业务信息安全评估指南

YD/T 3627-2019 5G数字蜂窝移动通信网 增强移动宽带终端设备技术要求（第一阶段）

YD/T 3628-2019 5G移动通信网 安全技术要求

YD/T 3802-2020 电信网和互联网数据安全通用要求

YD/T 3956-2021 电信网和互联网数据安全评估规范

YD/T XXXX-202X 5G数据安全总体技术要求

3 术语和定义

GB/T 25069-2010、GB/T 35273-2020、YD/T XXXX-202X界定的术语和定义适用于本文件。

4 略缩语

下列缩略语适用于本文件。

5GC	5G 核心网	5G Core
5G-RAN	5G 无线接入网络	5G Radio Access Network
AMF	接入和移动管理功能	Access and Mobility Management Function
IP	互联网协议	Internet Protocol
IPSec	互联网安全协议	Internet Protocol Security
MAC	媒体访问控制	Media Access Control
MANO	编排与管理	Management and Orchestration
MEC	移动边缘计算	Mobile Edge Computing
NAS	非接入层	Non Access Stratum

NF	网络功能	Network Function
NFV	网络功能虚拟	Network Functions Virtualization
NRF	网络存储功能	Network Repository Function
NSSAI	网络切片选择辅助信息	Network Slice Selection Assistance Information
SDN	软件定义网络	Software Defined Network
SSL	安全套接字协议	Secure Sockets Layer
TLS	传输层安全性	Transport Layer Security
UDM	统一数据管理	Unified Data Management
VLAN	虚拟局域网	Virtual Local Area Network
VNF	虚拟化网络功能	Virtualized network function
VPN	虚拟专用网络	Virtual Private Network

5 概述

5.1 评估总体框架

5G 数据安全评估通过文件查验、系统演示、测评验证、人员访谈等方法，针对 5G 业务数据安全、终端设备数据安全、无线接入数据安全、核心网数据安全、5G 基础设施数据安全以及通用数据安全等，明确评估方法和评估要点，引导提升 5G 数据安全水平。评估框架如图 1 所示。

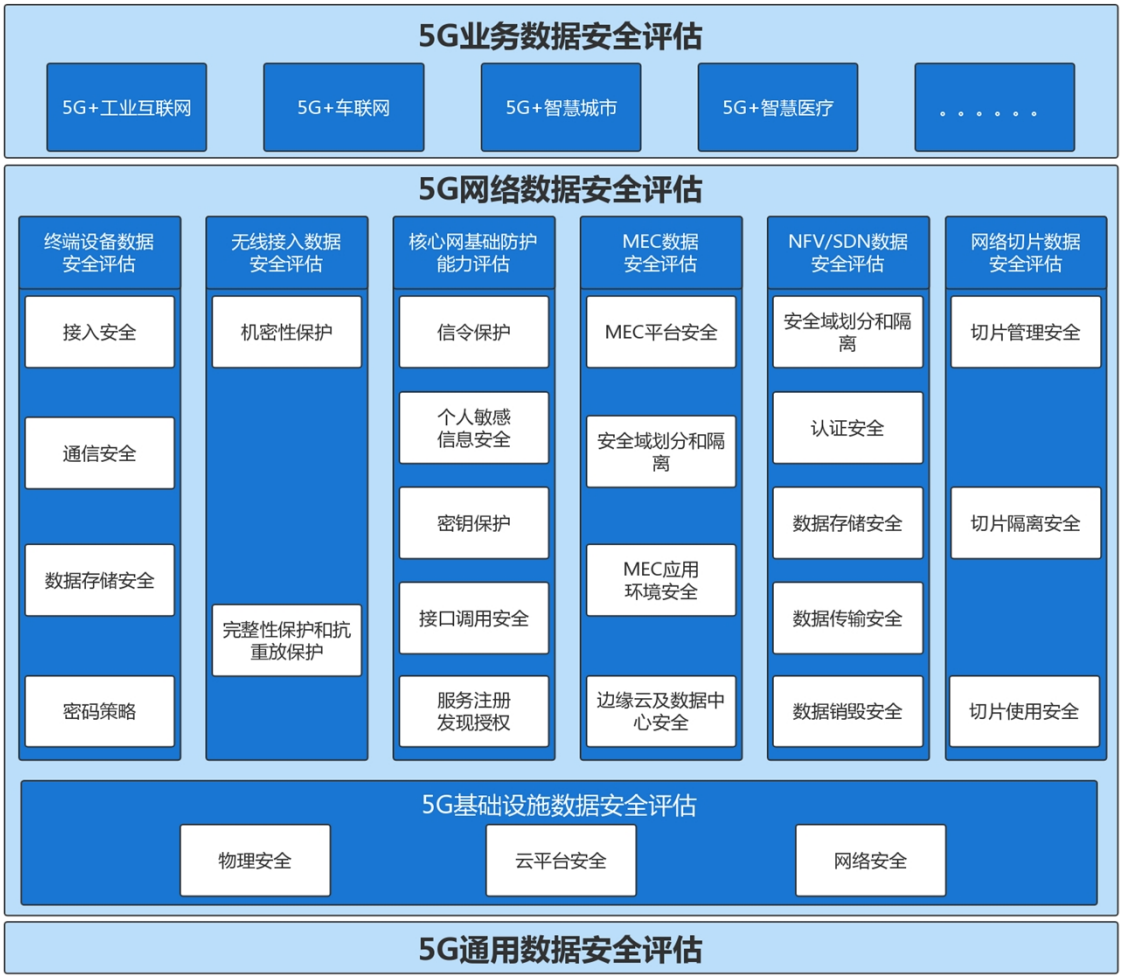

图 1 5G 数据安全评估框架

5.2 评估原则

标准性原则：遵循相关标准规范开展 5G 数据安全评估。

可重复和可再现原则：在相同的环境下，对同一评估对象，不同的评估人员依照同样的要求，使用同样的方法，对每个评估实施过程的重复执行都应得到同样的评估结果。

可控性原则：在评估过程中，应保障参与评估的人员、使用的技术和工具、评估过程都是可控的。

最小影响原则：从相关管理层面和工具技术层面，将安全评估对 5G 数据以及承载数据的应用、系统、网络正常运行的可能影响降到最低限度。

保密原则：评估人员开展5G数据安全评估工作前，需要与被评估对象就数据安全保密责任义务进行认定与划分，包括签署保密协议、做出保密承诺等，并对评估中获取的相关信息、评估过程文档等严格保密。

5.3 评估启动条件

满足下列情形之一，应及时启动5G数据安全评估：

a）5G网络建设、运维阶段应开展数据安全评估的；

b）5G新业务上线前（含合作推广、试点、试商用）应开展数据安全评估的；

c）5G业务运营阶段，其数据承载环境发生较大变化（如数据采集渠道变更、数据存储系统升级改造、数据处理技术变更等），应开展数据安全评估的；

d）开展与5G网络、应用和平台相关的数据活动（如开放数据对外接口、数据共享、数据转移、数据加工、数据出境等）前，应开展数据安全评估的；

e) 行业主管部门要求进行5G数据安全评估的；

f）满足国家法律法规有关情形，应开展5G数据安全评估的。

5.4 评估实施流程

5.4.1 评估准备

为保证评估的有效进行，在开展评估之前，评估团队与被评估对象需进行相应的评估准备工作。具体如下：

a）组建评估团队

应组建适当的5G数据安全评估团队，评估人员需具备数据安全评估相关能力，以支撑整个评估过程的推进及有效开展。当被评估对象委托安全服务机构开展5G数据安全评估时，应与被委托单位共同组建评估团队。

b）准备评估环境

要求被评估对象根据评估团队提供的评估清单进行对应的评估环境准备，并对评估环境进行充分有效的说明，以保证评估有效顺利开展。

c）确定评估范围

评估团队根据5G数据评估对象进行评估范围和对象界定，明确被评估对象涉及5G数据安全的相关终端、系统、平台、应用等范围。

d)评估对象调研

评估团队应对被评估对象5G数据安全相关工作进行充分调研，调研内容包括5G数据安全管理相关的制度流程、数据安全保障措施、业务运营情况等。

5.4.2 评估实施

评估实施过程中，评估团队可采取文档查验、人员访谈、系统演示、测评验证等方式对管理措施和技术措施进行评估，对不合规项逐项提出针对性整改建议。评估团队应当对评估佐证材料进行收集、整理，做好评估过程记录。被评估对象在评估过程中应积极配合评估机构的工作，制定整改计划，并及时对评估过程中出现的问题进行整改。5G数据安全评估方法包括以下几种：

a） 文档查验

文档查验是指评估人员查阅5G数据安全相关文件资料，以评估5G数据安全管理制度文件是否符合标准要求的一种方法。通常在评估准备阶段以及5G数据安全管理类评估部分使用该方法，被评估对象需要事先完整准备上述文档以供评估人员查阅。

b）系统演示

系统演示是指被评估对象相关人员开展演示，评估人员查看承载5G数据的应用、系统、网络，包括数据采集界面、数据展示界面、数据存储界面、数据操作日志记录等，以评估5G数据安全保障措施是否有效的一种方法。在评估实施阶段，被评估对象需安排相关技术操作人员进行现场演示，评估人员根据系统演示情况进行查验。如系统存在保密性要求，评估可通过事后提供日志列表或测试环境等方式进行。

c）测评验证

测评验证是指评估人员通过实际测试承载5G数据的应用、系统、网络，查看、分析输出结果，以评估5G数据安全保障措施是否有效的方法。在评估实施阶段，评估人员可使用该方法对数据全生命周期涉及的相关技术指标进行验证，评估人员需要事先进行业务注册、准备验证工具等以完成相关评估。

d）人员访谈

人员访谈是指评估人员通过与被评估对象相关人员进行交流、讨论、询问等活动，以评估数据安全保障措施是否有效的一种方法。在评估实施阶段，被评估对象需安排熟悉5G数据流转过程，以及熟悉承载5G数据应用、系统、网络运行情况的人员参加访谈。

评估实施阶段包括初评、复评两部分：

a）初评：指评估团队在完成评估准备工作后，对评估对象开展的初步评估。评估团队应根据初步评估结果，结合评估对象实际情况，给出初评结论并对评估不合规项逐项提出针对性整改建议。

b）复评：指评估团队在被评估对象完成整改或达到整改期限后，对整改情况进行的复核评估。评估团队应根据初评结论及整改建议,检查与复核被评估对象的整改措施是否符合或达到整改建议的要求，是否已经消除风险项，并给出复评结论。

5.4.3 评估总结

在评估总结阶段，评估团队对评估实施阶段中的评估建议以及评估整改落实情况进行核验，确认被评估对象已经配套数据安全管理措施和数据安全技术措施并满足YD/T XXXX-202X相关要求，形成5G数据安全评估总结报告。

6 5G业务数据安全评估

6.1 5G业务通用数据安全

依据YD/T XXXX-202X 6.1、YD/T 3802-2020 7.1和YD/T 3169-2020 7.4相关要求开展评估。

6.2 5G垂直行业数据安全

6.2.1 行业应用数据安全

5G垂直行业应用数据安全评估，除依据本文件6.1相关要求开展，还应依照5G具体垂直行业及重

点场景（如5G+高清直播、5G+VR/AR、5G+云游戏等）下的特定数据风险识别和管理要求开展。

6.2.2 个人信息和重要数据

【文档查验】查验个人信息和重要数据安全管理制度，是否具有信息收集相关规定，是否符合信息收集的合法性要求和最小必要原则，是否制定隐私政策，是否说明收集、使用目的及所涵盖的各个业务功能，收集个人信息时是否进行告知。

【文档查验】查验数据使用管理制度，是否明确个人信息和重要数据存储、传输、加工、共享和使用的安全措施（包括脱敏、加密、安全检查、合规性风险评估及授权等）。

【文档查验】查验数据销毁管理制度，是否结合数据分类分级管理制度和安全需求建立数据销毁安全策略和操作规程。

【测评验证】通过技术验证数据销毁后是否不可恢复。

涉及个人敏感信息的，依据 GB/T 35273-2020中5.4、6.3、7.3、7.4、7.5和7.7相关要求、YD/T 3628-2019中5.5相关要求、YD/T 2692-2014中4.5相关要求开展安全评估。

6.2.3 不良信息和违法违规内容

【文档查验】查验5G垂直业务针对不良信息和违法违规内容的管理规定和监测处置记录，是否制定识别和停止发布不良信息和违法违规内容的管理规定，是否及时处理并按要求留存日志。

【系统演示】查验不良信息和违法违规内容样本库和管理日志，是否具有不良信息和违法违规内容样本库并定期更新。

【测评验证】结合垂直行业特点，通过技术验证5G垂直业务是否启用不良信息和违法违规内容识别和处置流程并按要求留存日志，对判定的不良信息和违法违规业务是否及时进行过滤、下架等处置。

7 MEC数据安全评估

7.1 MEC平台

依据YD/T XXXX-202X中7.1相关要求开展评估。

【测评验证】通过技术验证MEC平台是否对部署在较弱控制区域的MEC节点采取安全加固措施，MEC平台与部署在较弱控制区域的MEC节点之间的数据存储和传输是否具有安全保护措施，当MEC接口支持可信计算等技术时，逐级验证系统启动到上层应用全过程，MEC平台是否完整可信。

【系统演示】查验产品资料，同质化MEC之间是否建立了“MEC 资源池”，且资源池中MEC节点相互之间是否能提供容灾能力。

【测评验证】出现不可抗的外部事件时（可通过杀死关键进程、网元下电等技术手段进行模拟），是否可以快速切换到其他MEC节点，是否能够保障用户数据的可用性和业务连续性。

7.2 安全域划分和隔离

依据YD/T XXXX-202X中7.2相关要求开展评估。

【系统演示】查验产品资料和安全域划分策略，是否对系统划分不同的安全域并实施域间安全隔离(包括物理隔离、虚拟机隔离、网元隔离、网络隔离、数据隔离、流量隔离等)，是否为不同安全等级的系统或应用划分不同的安全域并实施域间安全隔离措施。

【系统演示】演示跨安全域互联访问、数据流转，是否具备在安全边界进行访问控制的技术手段(如接入鉴权、接入策略设置等)。

【测评验证】通过技术验证安全域内设备和应用数据访问与传输相关安全策略是否有效，是否对安全域内业务通信、数据流转采取必要的加密和身份识别措施。

7.3 MEC 应用环境

依据YD/T XXXX-202X中7.3相关要求开展评估。

【测评验证】通过技术验证 MEC 通信接口安全机制是否有效，MEC 平台与其他外部交互设备(包括 MEC 编排器、基站、核心网设备、用户设备等)以及 MEC 平台与运行在平台之上的应用程序之间是否支持认证机制。

【测评验证】通过技术验证访问控制权限是否按最小授权原则进行划分，每个应用关联账号是否仅能访问自身应用数据，MEC 平台管理员账号是否无权访问应用数据，应用是否仅能执行业务所需的必要操作。

【测评验证】当MEC支持动态身份标识、匿名化等技术，以削弱MEC计算节点标识和地理位置的映射关系时，通过技术验证处理效果，是否可防止第三方根据MEC节点位置推断用户的地理位置。

【系统演示】查验MEC平台的日志记录，是否记录第三方服务商的操作过程日志。

【系统演示】演示MEC平台的隔离操作，是否支持不同应用资源隔离（如虚拟处理器调度安全隔离、内存资源安全隔离），是否对无线接入域、核心网域、管理域、互联网域、局域网域进行VLAN划分隔离。

7.4 边缘云及数据中心

依据YD/T XXXX-202X中7.4相关要求开展评估。

【系统演示】演示边缘云和数据中心涉及的敏感数据处理、存储，敏感数据传输过程是否支持机密性和完整性保护（如TLS机制、IPSEC等），敏感数据存储是否支持加密。

【系统演示】演示边缘云和数据中心涉及的个人敏感数据或重要数据的使用，数据使用之前是否通过技术手段（如加密/匿名化）进行脱敏处理。

【测评验证】通过技术验证边缘云和数据中心为用户提供的数据访问权限，是否按照最小必要原则提供其所必需的、符合业务需求的数据。

【测评验证】通过技术验证边缘云和数据中心数据访问控制策略是否有效，是否对数据访问主体和客体实施身份验证和访问权限限制。

除上述要求外，边缘云及数据中心安全评估还需依据本文件7.1、7.2相关要求执行。

8 NFV/SDN 数据安全评估

8.1 安全域划分和隔离

8.1.1 安全域划分

【文档查验】查验云化VNF平台安全域划分与隔离制度，是否根据Hypervisor虚拟资源、接口流量、虚拟机/容器间流量、不同网络平面（用户面、控制面、管理面）安全隔离的需要，梳理不同的安全域清单，是否明确安全域划分策略，安全域划分是否充分考虑了平台网络规划设计、部署、维护管理和运营中的安全风险。

【系统演示】演示 Hypervisor 软件，是否提供不同虚拟机之间的 CPU、内存、磁盘 IO、网络间的隔离；在 Hypervisor 对内存进行重新分配时，是否对内存做清除处理。

【测评验证】通过技术验证 Hypervisor 接口，是否严格限定管理虚拟机所需的 API，是否不开放无关的协议端口，是否禁用 IP 转发、禁用响应广播请求、禁止接受/转发 ICMP 重定向消息等功能。

【系统演示】演示虚拟机采用的安全组、VLAN 隔离、虚拟防火墙、虚拟安全网关等方式，是否实现虚拟环境边界防护，是否防止跨租户之间的非授权访问及数据泄露。

【测评验证】通过技术验证某个虚拟机崩溃后是否影响其他虚拟机的运行。

【系统演示】演示虚拟机生命周期检查，长时间不上线的虚拟机是否做环境隔离。

【测评验证】通过技术验证安全域边界访问控制措施，是否对安全域跨域行为进行监控和审计。

8.1.2 跨安全域管理

【文档查验】查验跨安全域管理制度文件和日志记录，是否建立对跨安全域互联访问的管理流程，是否定期梳理互联访问策略。

【测评验证】通过技术验证安全域间接口的设备鉴权和认证能力，是否对不同安全域间的数据流转进行鉴权和访问控制，是否实施数据流转流程控制和关键操作日志管理（包括跨域接口名称、跨域接口参数、跨域接口安全要求等内容）。

除上述要求外，云化 VNF 平台需要划分安全域并进行管理时，安全域中的虚拟机、虚拟网元等资源部署方案的安全评估需依据本文件 7.2 相关要求执行。

8.2 认证

8.2.1 认证规范

【系统演示】演示 NFV/SDN 安全管控机制，是否采用认证方式对虚拟化平台进行安全管控。

【文档查验】查验管控平台与虚拟化平台的统一认证机制、相关管理制度和日志记录，是否明确管控平台的账号开通、使用、销毁、权限分配等安全保障原则和审批流程要求，是否明确认证账号操作的审批要求和操作流程，是否建立并定期更新管控平台权限分配表,是否对管理员或超管账号进行定期梳

理，并对岗位角色的权限进行规范。

【测评验证】通过技术验证管控平台对虚拟化平台的认证能力，是否满足规划设计的认证机制。

8.2.2 授权管理

【系统演示】演示 NFV/SDN 安全管控机制，是否采用授权方式对虚拟化平台进行安全管控。

【测评验证】通过技术验证管控平台系统账号权限分配,每个账号是否按照角色或用户组进行授权，是否严格控制超级管理员账号数量。

8.2.3 账号管理

【系统演示】演示 NFV/SDN 安全管控机制，是否采用账号管理方式对虚拟化平台进行安全管控。

【系统演示】演示管控平台账号全生命周期管理流程，开发运维人员、第三方人员在创建和注销系统账号时，是否严格遵循系统账号创建和注销申请审批流程，是否记录审批过程和结果。

【测评验证】通过技术验证管控平台身份认证和权限控制机制，是否通过基于 IP 或 MAC 地址、账号口令的方式等，对所有接入或访问管控平台的用户、业务进行身份认证和权限控制。

【测评验证】通过技术验证管控平台账号锁定策略，是否对系统账号口令输入尝试次数进行限制。

【测评验证】通过技术验证管控平台口令管理策略，是否配置口令复杂度策略（如：口令长度不少于 8 位，使用大写字母、小写字母、数字及特殊字符中至少三种的组合，且与用户名、字符顺序无相关性），是否对口令遗忘的申请和重置流程实施严格管理，口令重置流程是否存在业务逻辑设计缺陷，是否留存申请和重置记录。

【系统演示】演示管控平台是否采取掩码显示、加密传输、加密存储等方式保护账号口令安全。

注 1：若采用哈希加盐的方式进行口令保护，盐值也需安全存储。

注 2：加密密钥是指一种用于控制密码变换操作（例如加密、解密、密码校验函数计算、签名生成或签名验证）的符号序列。[GB/T 25069-2010,定义 2.2.2.106]

8.3 数据存储

依据YD/T XXXX-202X中8.3相关要求开展评估。

【测评验证】通过技术验证MANO对各实体的管理，是否针对MANO中的证书、私钥、VNF访问口令、简单网络管理协议口令等敏感数据部署相应数据保护措施，SDN控制器是否对口令、私钥、流表、策略等敏感数据部署相应的数据保护措施。

【文档查验】查验数据存储制度，是否结合数据分类分级策略和管理要求明确数据存储安全策略和操作规程，是否具有数据存储系统差异化的安全存储保护手段（如加密、访问控制、数字水印、数字签名等）、数据存储介质安全策略和管理要求等。

【文档查验】查验存储的原始数据（如证书、口令等），是否按照安全级别进行差异化加密存储。

【系统演示】演示数据存储过程，是否部署完整性校验功能。

【测评验证】通过技术验证存储能力，如篡改敏感数据后是否能触发完整性校验。

8.4 数据传输

依据YD/T XXXX-202X中8.4相关要求开展评估。

【测评验证】通过技术验证MANO各实体间通信和SDN控制器南、北向接口数据传输等跨地域、跨数据中心的对传输安全有较高要求的数据传输场景，是否采用传输通道或数据加密模式（如采用TLS/SSL协议进行数据加密传输，或建立VPN加密传输通道方式行安全传输）。

【系统演示】演示NFV/SDN平台审核和监控能力，是否对数据传输安全策略变更进行审核和监控，是否对通道安全配置、密码算法配置、密钥管理等保护措施进行审核及监控。

8.5 数据销毁

依据YD/T XXXX-202X中8.5相关要求开展评估。

【测评验证】通过技术验证数据销毁效果，虚拟机在迁移或弹性扩缩过程中的数据销毁方法和技术是否有效，数据及其副本是否以不可逆方式销毁，数据销毁后系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配前是否得到完全清除并不可恢复。

【文档查验】查验数据销毁管理制度和日志记录，是否制定数据存储介质销毁监管措施，是否设置销毁监督角色监控销毁介质登记、审批、交接等过程，是否对销毁过程进行记录并形成数据销毁报告。

【系统演示】 演示数据销毁流程，是否依据数据存储介质、存储内容的重要性明确不同的销毁方法和机制，是否对不同作用的存储介质提供不同的销毁措施，数据销毁后所涉及的资源是否进行回收并进行登记。

9 网络切片数据安全评估

9.1 切片管理

依据YD/T XXXX-202X中9.1相关要求开展评估。

【文档查验】查验隔离机制，是否在用户侧、行业应用侧设置隔离机制以实现网络与用户的安全隔离。

【系统演示】演示切片网络设计，是否按照服务等级协议提供高可靠切片服务，切片网络自身安全边界是否清晰，切片网络自身安全是否可控。

【系统演示】演示虚拟机/容器层面切片网元之间的隔离，当网络功能部署在虚拟机上时，不同虚拟机使用的虚拟内存和磁盘是否没有重叠，释放的内存和磁盘是否具备强擦除的能力。

9.2 切片隔离

依据YD/T XXXX-202X中9.2相关要求开展评估。

【系统演示】演示切片隔离机制，是否对不同虚拟机之间共享同一存储资源设置数据隔离（例如VLAN、独立数据库等），虚拟机是否无法直接或间接访问其它虚拟机的数据。

【系统演示】演示访问控制流程，是否对控制面或用户面进行存储资源访问控制，包括强身份认证和细粒度授权（如对数据库的访问可控制到表、列级别）。

【系统演示】演示存储加密流程，是否根据不同的数据安全级别采用不同的存储加密机制，是否对核心关键数据进行加密存储并进行完整性验证。

【文档查验】查验数据备份恢复管理制度和日志记录，是否包括数据备份的规范和操作规程，是否明确规定数据备份的周期、备份方式、备份地点规范，是否对数据恢复性验证机制进行明确说明。

【系统演示】演示当数据发生丢失或破坏时，是否能利用备份进行数据恢复。

【文档查验】查验虚拟机迁移管理制度和日志记录，虚拟机迁移后是否具有存储资源销毁安全保护措施和记录。

【测评验证】通过技术验证虚拟机迁移后存储资源销毁效果，被销毁数据是否彻底删除，数据是否无法被非法恢复。

【测评验证】通过技术验证切片NF是否通过基于账号口令、密钥等方式对接入的其他切片的NF进行身份认证和权限控制，是否能够禁止未经授权的一个切片的NF访问另一个切片的NF服务。

【系统演示】演示网络切片隔离，网络切片之间是否具有端到端安全隔离机制（如：PRB、FlexE等隔离技术实施方案）。

9.3 切片使用

依据YD/T XXXX-202X中9.3相关要求开展评估。

【系统演示】演示行业应用认证、授权机制，在5G网络已有的用户认证鉴权基础上是否对切片用户端设备进行二次接入认证和授权。

【测评验证】通过技术验证鉴权、授权机制，是否使用双向鉴权、授权机制，切片管理及切片网络间通信是否使用安全协议（例如TLS、IPSEC）以保证通信的完整性、机密性以及抗重放。

【测评验证】通过技术验证切片模板、配置的检查与校验机制，是否能够防止由于错误配置导致切片的访问失效、数据传输与存储安全风险等。

【测评验证】通过技术验证切片运维权限管理，在切片运维管理时是否能防止越权进行运维。

【文档查验】查验切片生命周期管理制度，是否制定行业应用安全有关的切片级用户认证机制以及个人敏感信息或重要数据保护机制。

【系统演示】演示依据NSSAI的切片管理能力，是否区分不同类型、不同用途的切片，是否能确保用户初始接入网络时NSSAI指示基站及核心网网元将其路由到正确的切片网元。

10 核心网基础防护能力评估

10.1 信令保护

根据 YD/T 3628-2019 中 5.5.1、5.5.2 相关安全要求开展评估。

【文档查验】查验产品资料，是否提供AMF、NAS信令加密与完整性安全机制说明,是否提供NAS的加密与完整性保护机制、NAS加密算法与完整性算法的配置说明。

【系统演示】演示NAS信令加密算法（需根据产品资料配置并启用NAS的加密保护机制），AMF是否满足YD/T 3628-2019中5.5.1相关要求。

【系统演示】演示NAS完整性保护算法（需根据产品资料配置并启用NAS的完整性保护机制），AMF是否满足YD/T 3628-2019中5.5.2相关要求。

10.2 个人敏感信息

【文档查验】查验产品文档或个人数据保护声明资料，是否明确5G核心网涉及处理、存储和使用个人敏感信息的网络实体和相关操作。

【系统演示】演示个人数据保护机制，个人数据处理场景是否依据数据最小化原则，采用访问控制、匿名化、加密保护以及用户许可等技术手段对个人敏感信息的请求、存储、传输、使用等操作进行隐私保护。

10.3 密钥保护

【系统演示】查验被评估对象UDM用于认证和安全联盟场的长期密钥使用场景及保护机制说明，UDM网元是否按照YD/T 3628-2019中5.7.1相关内容要求，为用于认证和安全联盟建立的长期密钥提供保护机制，并且长期密钥不会离开UDM的安全环境。

10.4 接口调用

【系统演示】演示接口认证机制，是否为网元/系统间接口调用、数据转发及网络节点间数据使用等过程提供认证以防止假冒身份发送伪造数据。

【系统演示】演示网元间接口访问控制措施，是否基于控制措施限制每类网元可访问。

【系统演示】演示网元与基础电信其他系统间管理接口涉及的数据操作，是否采用严控数据导出操作、禁用特权操作、金库模式管控等措施保障数据安全。

10.5 服务注册发现授权

【文档查验】查验5G网元产品资料或安全机制声明文档，是否提供服务化接口的机密性、完整性和抗重放防护机制、授权访问控制。

【系统演示】演示服务注册、发现、授权，基于NF服务的发现和注册是否支持机密性、完整性和抗重放保护（如通过支持TLS提供NF服务化通信的机密性、完整性和抗重放保护），NRF是否确保NF发现和注册请求经过授权。

11 终端设备数据安全评估

11.1 接入安全

依据 YD/T XXXX-202X 中 11.1 相关要求开展评估。

【系统演示】演示终端接入过程具体的接入鉴权流程，是否满足 YD/T 3627-2019 中 15.1、15.2 相关要求。

【系统演示】查验设备接入鉴权行为日志，是否包括终端标识、接入方式、鉴权时间、鉴权结果等信息。

11.2 通信安全

依据 YD/T XXXX-202X 中 11.2 相关要求开展评估。

【测评验证】通过技术验证通信路径安全能力，是否满足 YD/T 3627-2019 中 15.1、15.2 和 YD/T 3628-2019 中 5.2 相关要求。

11.3 数据存储

依据 YD/T XXXX-202X 中 11.3 相关要求开展评估。

【文档查验】查验终端数据加密存储和完整性验证机制、访问控制和安全隔离策略，以及数据备份、恢复和销毁策略，5G 终端设备数据存储安全是否满足 GB/T 34977-2017 中 7.2 相关要求。

【系统演示】对于特定行业应用安全需求高的 5G 终端设备，演示终端数据加密存储和完整性验证、

访问控制和安全隔离以及数据备份、恢复和销毁，是否满足 GB/T 34977-2017 中 7.3 相关要求。

11.4 其他

依据 YD/T XXXX-202X 中 11.4 相关要求开展评估。

【文档查验】查验移动智能终端密码保护策略，文件类用户是否具备数据授权访问策略，是否具备用户数据加密存储、彻底删除、转移备份和远程保护策略。

【系统演示】演示用户数据存储，用户数据的时间最小化、去标识化处理和个人敏感信息存储是否满足YD/T 2407-2013中5.6相关要求。

12 无线接入数据安全评估

12.1 机密性保护

依据 YD/T XXXX-202X 中 12.1 相关要求开展评估。

【系统演示】演示加密和完整性保护，5GC 和 5G-RAN 密钥是否满足 YD/T 3628-2019 中 5.1.3 相关要求，用户数据和信令数据的机密性保护是否满足 YD/T 3628-2019 中 5.3.2 相关要求。

12.2 完整性保护和抗重放保护

依据 YD/T XXXX-202X 中 12.2 相关要求开展评估。

【系统演示】演示数据的完整性保护和抗重放保护，是否满足 YD/T 3628-2019 中 5.3.3 相关要求，无线接入侧的个人敏感信息和重要数据是否具有完整性保护和抗重放保护。

13 5G 基础设施数据安全评估

13.1 物理安全

依据YD/T XXXX-202X中13.1相关要求开展评估。

13.1.1 机房、室外无线接入设备场地

【文档查验】查阅相关材料，是否具备网络安全等级保护证明材料。

【文档查验】查验机房、室外无线接入设备场地物理环境和管理记录，机房物理环境安全、室外无线接入设备场地物理环境安全是否满足 YD/T 1734-2009 中 7.2.4、7.3.4、7.4.4 相关要求。

13.1.2 通用服务器

【文档查验】查验相关证明材料，是否按照 YD/T 1729-2008 中 5.1、5.2 相关要求对 5G 移动通信网进行定级。

【文档查验】查验验收和安全管理记录，是否按照 GB/T 21052-2007 第 4、5、6、7 章相关要求落实相应级别的物理安全防护要求。

13.2 云平台安全

依据YD/T XXXX-202X中13.2相关要求开展评估。

【文档查验】查验云平台数据安全相关管理制度，所有客户信息的保护措施是否满足 GB/T 31167-2014 中 6.6 相关要求。

【系统演示】查验云平台访问控制策略与规程，用户标识与鉴别、设备标识与鉴别、标识符管理、鉴别凭证管理与反馈、密码模块鉴别、账号管理、访问控制和信息流控制等，是否满足 GB/T 31168-2014 中 7.1、7.2、7.3、7.4、7.5、7.6、7.8、7.9 和 7.10 相关要求。其中，密码模块鉴别是否满足 GB/T 37092-2018 中 5.2、5.3、5.4、5.5 相关要求。

13.3 网络安全

依据YD/T XXXX-202X中13.3相关要求开展评估。

13.3.1 安全域划分与隔离

依据本文件 7.2 相关要求开展安全评估。

13.3.2 访问控制

依据本文件第 10 章相关要求开展评估。

13.3.3 链路冗余及数据备份

【文档查验】查验相关技术资料，是否采取采用多路径冗余传输、网络关键节点冗余等方式防止因网络故障导致的数据传输受影响或传输中断。

【系统演示】演示数据备份，对于集中部署的数据存储，是否采用数据中心内数据备份、异地数据备份等机制提高数据可用性。

13.3.4 网络异常行为监测

【测评验证】通过技术验证网络异常行为监测，是否能发现并及时记录 5G 网络数据异常行为，是否能发现并及时记录连接异常、IP 异常和端口异常等信息，

【系统演示】查验网络节点数据传输行为监控记录，是否能展示数据向外发送的时间、目的地、内容等信息，是否能结合异常基线发现平台内部数据泄漏问题。

【测评验证】通过技术验证数据包，是否能通过分析数据包的内容特征和连接特征实现对网络扫描行为的监测。

14 5G 通用数据安全评估

5G 通用数据安全评估依据 YD/T 3956-2021 中 5.11、5.12 和第 6 章相关要求开展。